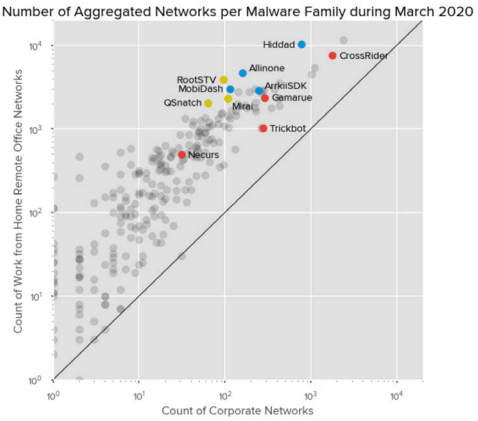
Travelers Cyber Risk Bulletin

Protecting Against Cyber Risks as Your Employees Return to Work

As work-from-home becomes return-to-work, you're doing everything you can to make sure your business is ready – for your employees and your customers. But is your business prepared to connect that work-from-home laptop safely back onto the company network, or is this the perfect opportunity that cyber criminals have been waiting for?

Home computer networks are typically considerably less secure than corporate networks. There is no dedicated IT staff to keep your routers patched and secure, and no matter how cautiously your employees browse the Internet, there may be others in the household who are prone to clicking on every tantalizing link.

A recent study by BitSight® Technologies showed just how unsafe home networks are. The chart below shows the prevalence of different malware families on home networks used by employees who are working remotely, compared to the corresponding corporate networks of their employers. In nearly every case, the specific malware was far more prevalent on the home network. For example, Trickbot — an infection that often precedes a crippling ransomware attack, was found 3.75 times more often on home networks than on the corresponding corporate network.



Notably, there has not been a similar increase in actual ransomware attacks since the widespread adoption of work-from-home policies. This makes some sense, because ransomware attackers would profit little from encrypting a single laptop of a work-from-home employee. But as soon as that laptop is put back onto the corporate network, the scope of potential damage that can be caused, together with the size of the ransom that can be demanded, increases dramatically. Is your business ready?

Travelers Cyber Risk Bulletin

Steps to Protect Your Network as Employees Return to Work

In the traditional "castle and moat" model of network security, firewalls and similar controls establish a perimeter around the corporate network. Computers inside the perimeter are trusted, and those outside are not. The more recent "zero trust" model of network security changes the paradigm, adopting the mantra "never trust, always verify." Most corporate networks fall somewhere on the spectrum between the two models. Therefore, they are at risk if cybercriminals secure a foothold on a work-from-home device that is then brought inside the perimeter. While it may not be possible to fully adopt zero-trust principles as employees return to work, there are steps that businesses can take to minimize the risk that cybercriminals are lurking on an infected laptop.

Update network devices and controls

With many businesses operating remotely or at a reduced capacity over the past months, there is a risk that critical components of your IT infrastructure may not have been kept up-to-date. Before bringing employees back into the office, be sure that all firewalls, servers, and other network components have been updated and properly secured.

Double-check your backups

Ransomware is one of the fastest growing trends in cybercrime right now. Businesses hit with ransomware may be unable to operate for weeks or even months. To mitigate the potential impact of a ransomware attack, take time to ensure that your backups are comprehensive — covering not just data, but also critical services such as Active Directory — and that your backups are stored in a segregated or off-site location that would be inaccessible if your network is compromised. For additional information on how to protect your business from ransomware, see our last *Cyber Risk Bulletin*, "Spotlight on Ransomware."

Ensure work-from-home devices have been updated

Unless your business has strong endpoint configuration controls, there is a risk that laptops and other work-from-home devices have not been updated. Before allowing these devices back onto your corporate network, make sure that they have received the latest patches and security updates.

Upgrade your defenses

Businesses that are using only antivirus on their network should give serious consideration to upgrading to an endpoint detection and response (EDR) solution. The latest EDR technologies provide far greater capabilities than traditional antivirus in protecting against attacks, monitoring for anomalous behavior on each system rather than simply searching for malware. Some EDR solutions, such as the SentinelOne™ platform, provide the ability to "roll back" a ransomware attack after it happens.

Have a plan

Even after taking all of these precautions, it is still possible that an employee could bring a compromised device inadvertently onto the corporate network. Be prepared for that possibility, by being extra vigilant for unusual network activity and by having an incident response plan in place.

To learn more about our cyber capabilities, visit travelers.com/cyber

TRAVELERS

travelers.com

Travelers Casualty and Surety Company of America. One Tower Square, Hartford, CT 06183